JC10 Rec'd PCT/PTO 1 4 NOV 2001

2/PRTS

09/926517

Method and apparatus for storing and retrieving PIN codes

This invention relates to a method and apparatus for storing and retrieving a number of personal identification numbers (PINs) for protected-access devices, in particular smart cards and magnetic stripe cards.

Nowadays many devices have protected access through personal identification numbers. PINs are granted in particular for smart cards, money cards, ID cards as well as access-protected software and the like. Access is only possible after the particular PIN code is entered. The PIN owner must remember the PINs so that only he can have knowledge of them. The constantly rising number of PINs to be remembered is a problem since human memory is limited and the PINs are usually not freely selectable and therefore difficult to remember.

EP-A-0 742 532 discloses a method and apparatus for storing and retrieving PIN codes easily and safely. The proposal is to store the secret PIN code in an externally unreadable primary memory and to store a freely selectable personal code more easily remembered by the PIN code owner in a secondary memory. If the PIN code owner has forgotten the secret PIN code he inputs the personal code into the apparatus, and if a comparison performed in a microprocessor matches the personal code stored in the secondary memory a display indicates for a predetermined time period the secret PIN code stored in the primary memory. A plurality of secret PIN codes can also be stored in the primary memory that are indicated on the display one after the other by means of the same personal code. EP-A-0 637 004 likewise discloses such a method at the end of the introduction to the description.

The solutions proposed in the prior art have the disadvantage that the owner of a plurality of secret PIN codes must remember not only the more easily remembered personal code but also at least which smart card or magnetic card the stored and retrieved secret PIN codes are to be assigned to. With the constantly increasing number of devices with protected access through PINs, this proposed solution is unsatisfactory.

The problem of the present invention is therefore to propose a method and apparatus for storing and retrieving a number of PIN codes by which a single, freely

selectable personal code permits retrieval of exactly the secret PIN code associated with the particular protected-access device.

This problem is solved by the features of the independent claims.

Unlike known systems for storing and retrieving a number of PIN codes, the invention provides for a unique feature of the particular associated protected-access device, for example the serial number of a smart card or an automatically measured property of the chip contained in the smart card, to be stored in addition to each stored PIN code. Between each stored PIN code and the associated stored unique feature of the particular device or smart card a unique firm link is generated. Upon retrieval of an individual PIN code for a protected-access device, two entries are made: firstly a previously freely selected access code which is the same for each retrieval process and therefore easily remembered, and secondly the unique feature of the protected-access device or smart card whose individual PIN is to be retrieved. The access code known only to the owner of the individual PIN guarantees that the individual PINs cannot be spied out by third parties. Entry of the unique feature is required in order to retrieve the associated individual PIN via the unique firm link. The individual retrieved PIN can then be indicated.

The inventive method and apparatus, through the particular linking of the secret PIN codes with the unique feature of the associated protected-access device, thus offer the advantage of permitting safekeeping and accurate retrieval of different PIN codes by means of a single, freely selectable access code.

For retrieval of the PIN code it is irrelevant whether the freely selected access code or the unique feature is entered first. The individual PIN is in any case outputted only if both the entered access code was permissible and the entered unique feature matches one of the stored unique features.

The access code and/or unique features and/or PIN codes are advantageously stored in encoded form. This makes it harder for a third party who has procured access to the memory areas to detect the relevant contents of the memories.

In a special embodiment of the method it is provided that the access code serves as a key for encoding the unique features and/or PIN codes and remains stored only as long as it is required for encoding said data. Upon retrieval of an indi-

vidual PIN the unique feature of that device whose individual PIN is to be retrieved is entered and encoded by means of the access code likewise to be entered, a comparison then taking place with the previously stored and identically encoded unique features. Comparison of the feature entered in encoded form with the feature stored in encoded form thus permits two tests to be performed simultaneously: firstly, whether the access code is permissible and, secondly, whether the entered unique feature matches one of the stored unique features. If the access code is impermissible or no corresponding unique feature is stored, the comparison turns out negative. If comparison turns out negative, a wrong PIN code not stored is outputted. If comparison turns out positive, the individual PIN code stored in encoded form is decoded with the entered access code and outputted. The access code is then deleted.

In order to increase the protection of the stored data from unauthorized access, the PIN codes can be encoded also - optionally in addition to the above-described encoding - by the particular unique feature of the protected-access device associated with the PIN code forming the key.

The PIN codes are kept most safely if the freely selected access code is only stored briefly, i.e. is no longer present after deletion, the stored unique features are present encoded with the access code, and the particular associated PIN codes are present encoded with the access code, on the one hand, and with the associated encoded unique feature, on the other hand. Decoding and subsequent outputting of the PIN codes then take place in the reverse order solely through entry of the access code and the particular unique feature of the protected-access device whose individual PIN code is to be retrieved.

The protected-access devices may be in particular smart cards and magnetic stripe cards. The unique feature of a magnetic stripe card may be for example its serial number, which must be entered manually in addition to the access code. In particular with smart cards, the unique feature may be not only the serial number but also a physical property characteristic of the particular chip. Such a physical property may be for example the data processing speed characteristic of each chip, which is determined using a defined algorithm. The time it takes the chip to execute the given algorithm serves as the unique feature of the smart card.

The inventive method can advantageously be carried out with a modified pocket card reader. Pocket card readers are used for reading the freely accessible data that are permanently stored in a smart card or variable. In particular in connection with money cards they are used for verifying the amount of money still stored in the money card. Such conventional pocket card readers are equipped merely with a keyboard for inputting the freely selected access code and PIN codes to be stored as well as optionally the serial numbers or other unique features of the associated cards, and software for carrying out of the above-described method for outputting and retrieving the PIN codes. If the unique feature is a characteristic physical property of the card which is detected automatically, the pocket card reader is equipped with a corresponding device. That is, the pocket card reader contains for example a program and device for executing an algorithm on the smart card and measuring the duration of execution of the algorithm.

Use of a pocket card reader has the advantage that it is very flat and has approximately the size of a smart card so that it can be taken along anytime.

In the following the invention will be explained by way of example with reference to the two figures, in which:

Figure 1 shows smart card 10 and pocket card reader 20 for introduction of smart card 10, and

Figure 2 shows the linking between memory areas *M*1 to *Mn* containing data on unique features with associated memory areas *PIN*1 to *PINn* in which the secret PIN codes are stored.

Figure 1 shows smart card 10 with chip module 12, writing box 11 and serial number 13. The smart card may be a money card or credit card or the like, and the entry of a secret PIN code is necessary before each access to a secret memory area of the chip in chip module 12 of smart card 10. The card can be inserted into pocket card reader 20 which is a little wider than smart card 10. For this purpose pocket card reader 20 has two platelike cover elements 21 and 22 interconnected at their edges 24 and forming between each other gap 23 into which smart card 10 is introduced, as shown by the arrow in Figure 1. If the card is a money card, conventional pocket card readers indicate the amount of money stored in the money card without

requiring the entry of a PIN code. If the user of the money card wants to increase the amount of money stored in the card at a bank machine, he must first input his PIN into the bank machine to be able to start the transaction. The card holder can store this PIN code in the pocket card reader with many other PIN codes so that he can retrieve them anytime, for example when he wants to perform a transaction for refilling the money card.

The method for storing and retrieving a number of PIN codes will now be described by the example of pocket card reader 20.

First, pressing button IN indicates to pocket card reader 20 that a freely selectable access code is to be inputted. The freely selectable access code is expediently inputted upon start-up of pocket card reader 20. It may also be provided that a plurality of users each having a plurality of smart cards use one pocket card reader. A plurality of access codes are then used, i.e. at least one access code per user.

Then the freely selectable PIN is inputted with the aid of numeric or alphanumeric keyboard 26 and subsequently confirmed by another pressing of button IN. The freely selectable PIN is stored at least for a short time period and henceforth used as the access code for the pocket card reader.

Next, a unique feature of smart card 10 is inputted into the pocket card reader and confirmed by pressing of button IN. The unique feature used may be for example serial number 13 of smart card 10. After entry of the unique feature the secret PIN stored in smart card 10 is inputted into the pocket card reader and likewise confirmed by pressing of button IN. One can also first input the secret PIN and then the unique feature of smart card 10. In any case display 25 leads the user through the program by indicating which information is to be inputted next. Figure 1 shows in display 25 that the secret PIN code is to be inputted next, which occupies first memory area *PIN*1 as explained in the following.

Figure 2 specifies memory areas *M*1 to *Mn* and *PIN*1 to *PINn*. The inputted unique feature of smart card 10, serial number 13 of smart card 10 in this example, is stored in memory area *M*1 and the associated PIN is stored in memory area *PIN*1. The two memory areas are firmly linked together, as indicated by the double arrow. The storage process is thus ended. In the described way further unique features *M*2

to *Mn* can be stored with firmly associated personal identification numbers *PIN*2 to *PINn*. Memory areas *M*1 to *Mn* and *PIN*1 to *PINn* are externally inaccessible or unreadable. This also applies to the memory area in which the access code is stored.

Retrieval of a special stored PIN takes place analogously. Pressing button OUT indicates to pocket card reader 20 that an individual PIN is to be read. Pocket card reader 20 then asks the user to enter the access code, on the one hand, and enter the unique feature of the smart card whose individual PIN code is to be retrieved, on the other hand. In the above-described example, serial number 13 of smart card 10 is entered as the unique feature. After pocket card reader 20 has tested and confirmed the permissibility of the access code and after a comparison of the entered feature with the unique features stored in memory areas *M*1 to *Mn* has yielded a positive result in pocket card reader 20, display 25 indicates the individual PIN code associated with the unique feature found, i.e. the PIN code stored in memory area *PIN*1 in this example. The display ends after a few seconds, for example approximately 3 seconds, or after the card has been withdrawn from the pocket card reader.

If the entered access code was inadmissible or no stored unique feature can be found for the entered unique feature, display 25 indicates a PIN code that matches none of the PIN codes stored in memory areas *PIN*1 to *PINn*, alternatively indicating an error message

In the above-described embodiment a unique feature of a smart card is linked with the PIN associated with said smart card by particular memory areas *M*1 and *PIN*1, *M*2 and *PIN*2, ... *Mn* and *PINn* being firmly associated with each other. In an alternative embodiment, the data are linked by each stored secret PIN being encoded with the associated unique feature. Upon an attempt to retrieve the PIN stored in encoded form, the PIN stored in encoded form is decoded by means of the same unique feature. The linked memory areas are thus not hardwired but logically combined.

According to another embodiment of the invention it is provided that the freely selected access code is only stored temporarily. The access code must only remain stored as long as it is required for encoding the associated unique feature and optionally the individual PIN upon storage of individual PINs. After entry of a unique

feature and the associated PIN, encoding of the unique feature and optionally the individual PIN with the access code, and storage of the encoded unique feature and optionally encoded individual PIN, the unique feature and the individual PIN are present in encoded form in the particular memory areas, while the access code used as a key is deleted. This ensures that anyone able to procure access to the individual memory areas without knowledge of the access code cannot interpret the contents of the memory areas.

At the beginning of retrieval of an individual PIN the access code and the unique feature of the smart card whose individual PIN is to be retrieved are inputted via keyboard 26. Then the inputted unique feature is encoded with the access code and it is then tested whether there is a counterpart to the thus encoded unique feature in memory areas *M*1 to *Mn* where the unique features of different smart cards were previously stored in encoded form. If this test yields a positive result, the PIN code linked therewith is indicated on display 25, optionally after decoding by means of the access code.

Card 10 need not be a smart card but may also be a magnetic stripe card for example. The invention is equally applicable thereto. If a smart card is involved, however, it is expedient to use an automated method for entering the unique feature. Instead of inputting a unique feature like the serial number via keyboard 26, the pocket card reader can also automatically determine a characteristic property or serial number of chip 12 contained in smart card 10 and use it as the unique feature. In the case of money cards for example, data transfer already takes place between pocket card reader 20 and chip 12 of smart card 10 in order to permit indication of the amount of money stored in the smart card. It is therefore readily possible to determine a characteristic physical property of the chip via the already realized contacting between chip 12 and pocket card reader 20. For this purpose, pocket card reader 20 causes an algorithm to be executed in chip 12, and the time it takes chip 12 to execute the algorithm is detected and used as the characteristic physical property of chip 12 and thus smart card 10. This process takes place automatically after smart card 10 has been inserted completely into gap 23 of pocket card reader 20 and the user of the pocket card reader indicates by pressing button OUT that he wants to

retrieve the individual PIN associated with said smart card. The card holder need only input the previously freely selected access code via keyboard 26 into pocket card reader 20 in order to start the above-described comparison method of the characteristic physical property and obtain the indication of the individual PIN associated with card 10 on display 25. Any property may serve as a characteristic physical property if it is reliably detectable and specific to each card or its chip.

In principle, the automatic method for determining the unique feature as described above for a smart card is also possible with a magnetic stripe card which also has unique features like serial numbers. However, the structure of a suitable pocket card reader is more elaborate than in the case described above for a smart card.